ИНФОРМАЦИОННЫЙ ДОКУМЕНТ

ЛАЗЕЙКИ ДЛЯ АТАК

ИССЛЕДОВАНИЕ ПОКАЗАЛО, ЧТО УСТРОЙСТВА ПЕЧАТИ УЯЗВИМЫ ДЛЯ КИБЕРАТАК

Заботясь о безопасности, ИТ-специалисты нередко забывают об устройствах печати.

Легкая мишень: многие сетевые печатающие устройства не имеют блокировок и ограничений доступа.

Это создает весомую угрозу. Устройства печати нуждаются в надежной защите, как и прочие устройства в корпоративной сети. Однако зачастую они оказываются беззащитны перед кибератаками и служат лазейками, через которые злоумышленники воруют финансовые и конфиденциальные данные, что губительно для бизнеса.

Компания Spiceworks провела опрос, в котором участвовало более 300 специалистов, ответственных за принятие решений в сфере ИТ. Оказалось, тех, кто считает, что устройства печати нуждаются в серьезной защите, всего 16% — гораздо меньше, чем тех, кто заботится о безопасности настольных компьютеров, ноутбуков и мобильных устройств.[1] Это наглядно демонстрирует общепринятый подход к сетевой безопасности. О защите устройств печати заботятся три из пяти организаций, однако тех, кто думает о безопасности других сетевых устройств, гораздо больше. Поэтому и получается, что устройства печати часто остаются уязвимы при наличии на рынке массы простых решений для их защиты.

В этом документе приводятся сведения о защите устройств печати, полученные в результате опроса Spiceworks, рассматриваются последствия взломов и перечисляются некоторые современные встроенные средства защиты от кибератак.

ТОЛЬКО 16% ОПРОШЕННЫХ СЧИТАЮТ, ЧТО УСТРОЙСТВА ПЕЧАТИ НУЖДАЮТСЯ В СЕРЬЕЗНОЙ ЗАЩИТЕ.[1]

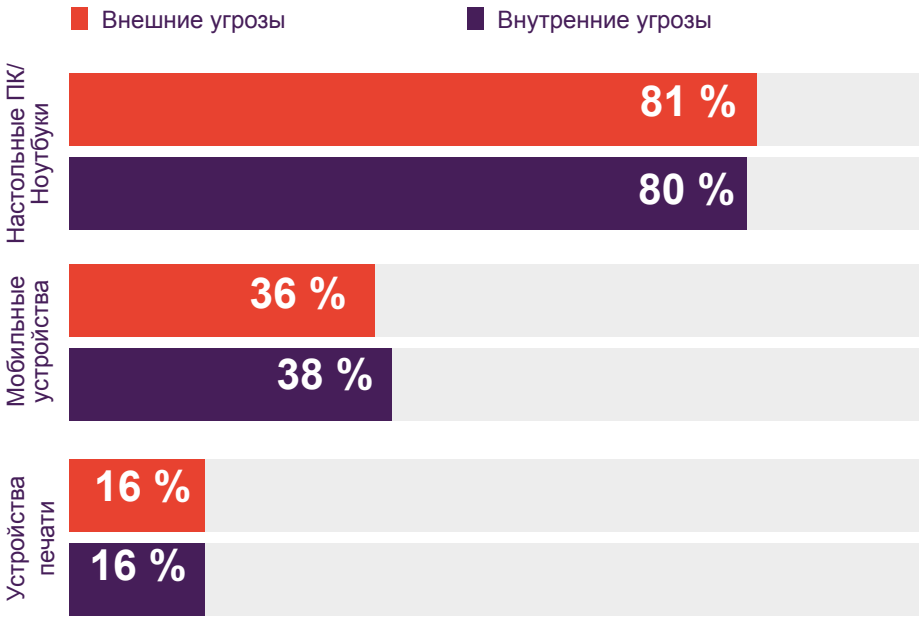
ЛАЗЕЙКА ДЛЯ АТАК

В ходе опроса Spiceworks 74% респондентов признали, что за последний год их организация в том или ином виде столкнулась с внешней ИТ-угрозой. 70% респондентов отметили, что источником проблем с безопасностью стала внутренняя причина, например пользовательская ошибка или использование персональных устройств, домашних и общедоступных сетей для рабочих целей.[1]

ГЛАВНЫЕ ВНЕШНИЕ ИТ-УГРОЗЫ

Вредоносное ПО | Вирусы | Фишинг

Главной мишенью для злоумышленников по-прежнему остаются настольные компьютеры и ноутбуки, однако мобильные устройства и устройства печати также находятся под угрозой.[1] На устройства печати теперь приходится 16% атак, что очень много по сравнению с 2014 годом, когда их было всего 4%, по данным Spiceworks. Реальная цифра может быть даже больше, поскольку устройства печати не столь тщательно проверяются, как компьютеры и мобильные устройства.



НА ПЕРИФЕРИИ ВНИМАНИЯ

Опрос Spiceworks наглядно показал, что защита устройств печати часто отодвигается на второй план.

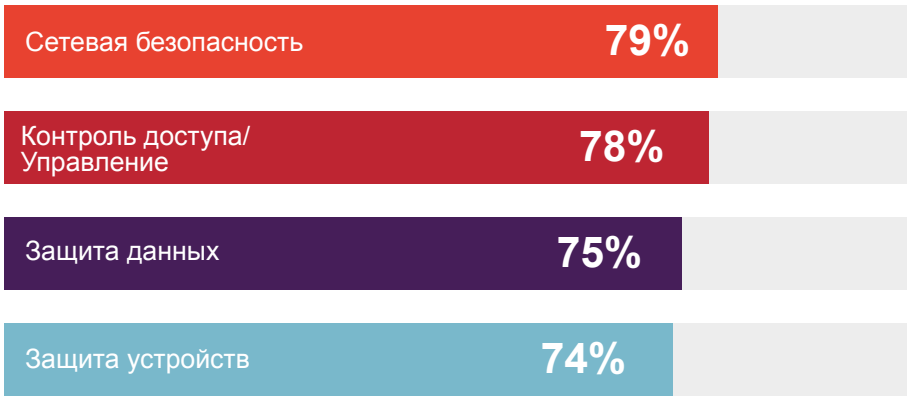
Все осведомлены, что нужно заботиться о безопасности сети, конечных устройств и данных. Три четверти респондентов имеют те или иные средства для контроля и управления доступом, системы сетевой безопасности, защиты данных и конечных устройств.[1]

Однако про устройства печати почему-то часто забывают. 83% респондентов используют средства сетевой безопасности на настольных компьютерах и ноутбуках, 55% — на мобильных устройствах, и только 41% — на принтерах.[1]

Разрыв еще более очевиден в применении средств защиты конечных устройств.

Менее трети респондентов (28%) устанавливают сертификаты безопасности на устройства печати, тогда как для компьютеров этот показатель составляет 79%, а для мобильных устройств — 54%.[1]

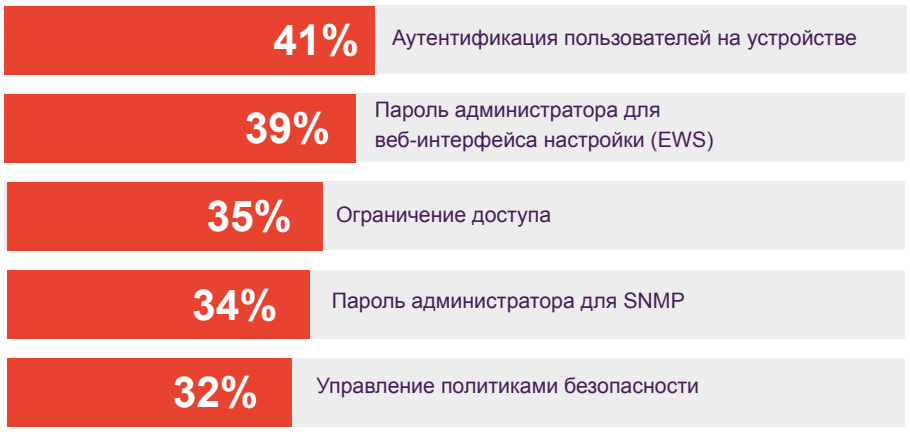
ОСНОВНЫЕ МЕТОДЫ ЗАЩИТЫ КОНЕЧНЫХ УСТРОЙСТВ



Среди наиболее популярных средств защиты конечных устройств к безопасности устройств печати имеют отношение защита документов, сетевая безопасность и контроль доступа, однако используют их менее половины респондентов.[1]

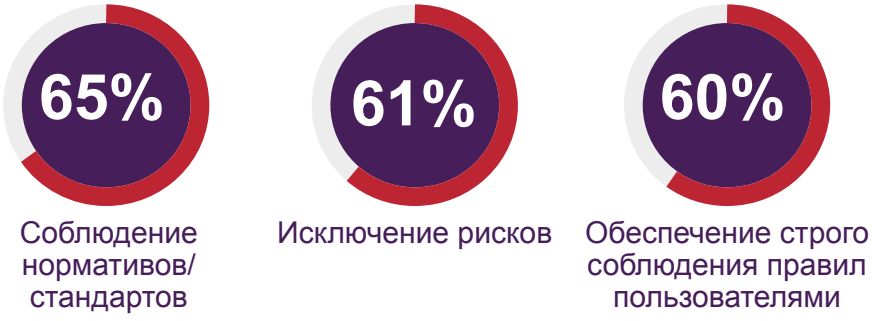
Специальные средства защиты устройств печати используются лишь в некоторых организациях, причем очень неравномерно. Только 40% организаций применяют аутентификацию пользователей, менее 40% защищают веб-интерфейс настройки с помощью паролей администратора.[1] Однако для надежной защиты требуется использовать оба этих способа и еще ряд других.

ОСНОВНЫЕ МЕТОДЫ ЗАЩИТЫ УСТРОЙСТВ ПЕЧАТИ



Что касается общих требований и методов проверки, с устройствами печати дела опять же обстоят гораздо хуже, чем с другими конечными устройствами. Почти в 90% организаций имеется политика информационной безопасности, однако она, как правило, не охватывает устройства печати. Например, 57% респондентов отметили, что используют средства защиты от вредоносных программ на компьютерах, и только 17% — в устройствах печати.[1]

ПОЧТИ 9 ИЗ 10 ИТ-СПЕЦИАЛИСТОВ НАЗВАЛИ СЛЕДУЮЩИЕ ПРИЧИНЫ, ВЫНУДИВШИЕ ИХ ВНЕДРИТЬ ПОЛИТИКУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:



Очевидно, что организации не считают защиту устройств печати чем-то необходимым. А зря.

«На многих устройствах печати оставлены стандартные пароли, или вообще паролей нет, или используется один пароль для всех, — предупреждал в июньском выпуске Computerworld Майкл Ховард, главный консультант HP по безопасности. — Принтер, не защищенный паролем, — легкая добыча для мошенников. Они взламывают его и получают доступ ко всем документам, отправляемым на печать, — это так называемые атаки с помощью посредника. Так, они могут просматривать все, что печатает генеральный директор».[2]

ВОЗМОЖНЫЕ ПОСЛЕДСТВИЯ ВЗЛОМА УСТРОЙСТВ ПЕЧАТИ

По мнению старшего аналитика электронных угроз Bitdefender Богдана Ботезату, устройства печати представляют серьезную потенциальную брешь в системе безопасности. «В результате многочисленных телеметрических измерений в наших лабораториях по оценке уязвимостей, мы выяснили, что теперь самый беззащитный элемент сети — не маршрутизатор, а устройство печати».[3]

Такая уязвимость может дорого обойтись бизнесу. Одно незащищенное устройство печати делает уязвимой всю сеть: через него злоумышленники могут получить доступ к любому сетевому устройству, что подрывает безопасность сети.

Все понимают, чем грозит нарушение защиты. В ходе опроса Spiceworks респонденты назвали пять основных последствий:[1]

1. Растет число обращений в службу поддержки и время обслуживания

2. Падает производительность

3. Увеличивается время простоя

4. Увеличивается время вызовов

5. Ужесточаются правила для конечных пользователей

Однако последствия взлома устройства печати могут быть еще опаснее, особенно если речь идет об МФУ, рассчитанном на электронное хранение данных. Если злоумышленники доберутся до устройства печати, в кэше которого хранятся задания печати, то их добычей могут стать важные персональные или деловые данные.

Более того, через незащищенное устройство печати они могут зайти в корпоративную сеть и украсть номера социального страхования, финансовые данные, служебные записи или документы. Кража подобной информации сказывается не только на отдельных сотрудниках, но и на всей компании в целом, поскольку подрывает ее конкурентоспособность и вредит репутации.

ПРОСТОЕ РЕШЕНИЕ — ВСТРОЕННЫЕ СРЕДСТВА ЗАЩИТЫ

Очевидно, что следует заботиться о безопасности устройств печати. Некоторые печатающие устройства корпоративного уровня имеют удобные встроенные средства защиты, способные противостоять современным угрозам. Перечислим некоторые из них.

- Автоматическое обнаружение атак, защита и восстановление
- Контроль использования для предотвращения несанкционированных действий
- Простые дополнительные возможности для аутентификации при входе в систему, например PIN-код или смарткарты
- Устройство чтения бесконтактных карт для быстрой аутентификации
- Шифрование для печати важных документов

Устанавливая принтер или МФУ, обязательно изучите его встроенные средства защиты и активируйте их. Не стоит, подвергать себя опасности, когда можно легко настроить защиту. В Интернете вещей огромное количество точек доступа нуждается в защите — **пусть хотя бы безопасность устройств печати не будет для вас проблемой.**

НУЖНЫ БОЛЕЕ ЗАЩИЩЕННЫЕ УСТРОЙСТВА ПЕЧАТИ?

ПОДРОБНЕЕ ›

Источники:

1 Опрос 309 специалистов, ответственных за принятие решений в сфере ИТ, в Северной Америке странах EMEA и APAC, проведенный Spiceworks по поручению HP в ноябре 2016 г.

2 «Printer Security: Is your company's data really safe?», *Computerworld*, 1 июня 2016 г. http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

3 «Printers Now the Least-secure Things on the Internet», *The Register*, 8 сентября 2016 г. http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/